UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,656	10/14/2003	W. Todd Daniell	190250-1300	5661

38823 7590 03/31/2008

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, LLP/
AT&T Delaware Intellectual Property, Inc.
600 GALLERIA PARKWAY, S.E.
SUITE 1500
ATLANTA, GA 30339-5994

EXAMINER	
FRINK, JOHN MOORE	
ART UNIT	PAPER NUMBER
2142	
MAIL DATE	DELIVERY MODE
03/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/685,656	DANIELL ET AL.	
	Examiner	Art Unit	
	JOHN M. FRINK	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6,11-14,16,17 and 19-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,6,11-14,16,17 and 19-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/11/2008 and 2/15/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 1/25/2008 have been fully considered but they are not persuasive.

2. Applicant begins by arguing claim 6, rejected under 35 USC 102(b) as being anticipated by Shipp. The claim, as amended, now includes language to claim "tokenizing the attachment". Applicant argues that Shipp does not show tokenizing an attachment. Applicant's argument is persuasive. However, Applicant's argument for the allowability of claim 6 is unpersuasive in view of the new grounds of rejection, necessitated by Applicant's amendment, made below.

3. Next, still regarding claim 6, Applicant argues that Shipp teaches away from tokenizing attachments when considering a spam probability. Though Shipp does not teach this feature, the Examiner does not agree that Shipp teaches away from this feature.

Paragraph 81 of Shipp states:

*If mail contains attachments, do not log (spam mail **currently** does not contain attachments).* (Emphasis added)

Shipp thus does not teach away from considering that spam email may contain attachments. Shipp notes, through the use of the word "currently", that spam email does not contain attachments, but also anticipates that spam emails not containing attachments may change in the future. Milliken, the reference cited to teach processing email attachments in relation to spam email, was filed more than a full year after Shipp.

Milliken clearly views the situation regarding spam emails containing attachments to have changed. Shipp, by specifically limiting their assertion that spam emails do not contain attachments to the current state in 2002, clearly does not teach away from a future consideration of spam email containing attachments at some other point in time.

Applicant's argument thus is not persuasive.

4. Next, regarding claims 23, 24 and 25, Applicant repeats the arguments addressed above relating to Shipp. These arguments thus are not persuasive for the reasons given above.

5. Applicant's next argues claim 1, rejected under 35 USC 103 in view of Shipp, Devine, Milliken, Anderson, Uuencode, Gordon and Sahami. Applicant repeats their argument regarding "tokenizing the attachment" related to Shipp, which was addressed above. Applicant also repeats this argument relating to Devine, Anderson, Uuencode, Gordon and Sahami. However, none of these references were cited to teach "tokenizing the attachment"; only Milliken was. Applicant's arguments thus are not persuasive.

6. Addressing Milliken, Applicant argues that Milliken disclosure is different than Applicant's relating to tokenizing attachment. Milliken discloses generating hash values of email messages, including separate hashes of the email text and the email attachment, and utilizing said hash values to determine if a message is spam ([10-13]). Applicant specifically argues that "generating hash values is different than tokenizing an attachment". However, Applicant provides no further proof for this assertion. Furthermore, Applicant's own Abstract in their Specification states that "tokenizing of these portions generates tokens that are representative of these portions". Applicant's

claim language also states "tokenizing the attachment to generate a token that is representative of the attachment." Milliken discloses generating a hash of a messages attachment and "determining whether the hash values match hash values associated with prior e-mail messages". Paragraphs 50 - 52 elaborate on the hashing process. Clearly the hashes of Millken are representative of the attachment (which is in this case the input into the hash function); else utilizing the hash in a comparison operation would be fruitless. Furthermore, hashes are inherently based on, and thus representative of, their input.

Finally, in claim 1, items E1 and E2, Applicant describes the "tokenizing" as "comprising generating a . . . hash of the attachment". Applicant's argument that Milliken's generating of a hash is different than Applicant's claimed "tokenizing" is thus not persuasive.

7. Still arguing claim 1, Applicant addresses the Gordon reference, stating that "Gordon fails to disclose 'determining a probability value for each of the generated tokens' as recited in claim 1". To support this argument, Applicant states "determining a probability associated with words in an email is completely different than performing actions to tokenize an attachment." However, the Examiner never argued or cited art to teach that "determining a probability associated with words" was similar to "performing actions to tokenize an attachment". Applicant's argument thus is not persuasive.

8. Still arguing claim 1, Applicant addresses the Sahami reference, arguing that Sahami teaches away from attachments as evidence that a message is not spam. However, Applicant provides no citation or indication of where such language or

teachings made be found in Sahami. Furthermore, Shipp, also cited in relation to claim 1, notes that at one point in time, attachments were not view as an indication of spam, but also notes that that was merely the current state; spam email constantly evolves and changes to attempt to bypass spam filtering applications. More recent art, such as the citied Milliken reference, show where spam indications have changed. This argument was further addressed above, and is unpersuasive for these reasons and the reasons given above.

9. Applicant next argues that claims 11 – 14 and 26 – 29 should be allowable based on prior arguments. However, this argument is not persuasive for the reasons given above.

10. Next, regarding claims 15 – 17 and 30 – 34, Applicant repeats their argument regarding Shipp not teaching tokenizing in relation to attachments and spam. Said arguments are not persuasive for the reasons given above.

11. Next, Applicant repeats the arguments already addressed relating to Shipp and Milliken, now relating to claims 31 and 32. Said arguments are not persuasive for the reasons given above.

12. Applicant next argues that claims 16 – 17 and 33 – 34, as well as 19 – 22 and 35 - 38 should be allowable based on prior arguments. However, this argument is not persuasive for the reasons given above.

Finally, Applicant argues the Examiner's statement

> *Furthermore, UUencoding is a prior art element, as shown in Uuencode and MIME FAQ, and thus UUencoding the 160-bit number is combining a prior*

art element (UUencoding) to known methods (the known methods shown by Shipp in view of Devine, Milliken and Anderson) to yield predictable results."

Applicant is arguing that the teachings of the cited references do not show subject matter that is "well known in the industry." However, all assertions relating to the above citation argued by Applicant have been supported by publicly available prior art, as is cited in the Office Action and cited clearly in the above statement. Applicant's argument thus is not persuasive. Furthermore, the statement cited above and argued by Applicant was utilized to show the obviousness aspect of a rejection under 35 USC 103, which does not require "commonality of subject matter to something of unquestionable fact". Furthermore, this was not asserted by the Examiner, and no "Official Notice", which may entail such requirements, was taken.

The fact that "combining prior art elements according to known methods to yield a predictable result" is language relating to reasons to arrive at a conclusion of obviousness, not a conclusion of "commonality of subject matter to something of unquestionable fact".

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter for the reasons given below in the 35 USC 112 written description rejection. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o).

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 30 and 32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, claims 30 and 32 are amended to reference tokenizing the "*entire* attachment".

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shipp (US 2004/0093384 A1) in view of Devine et al. (US 6,968,571 B2), hereafter Devine, further in view of Milliken et al. (US 2004/0073617 A1), hereafter Milliken, further in view of Anderson et al. (US 2004/0064537 A1), hereafter Anderson, further in view of Uuencode and MIME FAQ (http://web.archive.org/web/20021217052047/http://users.rcn.com/wussery/attach.html), further in view of Gordon et al. (US 6,732,157 B1), hereafter Gordon, further in view of Sahami et al. (A Bayesian Approach to Filtering Junk E-Mail), hereafter Sahami.

6. Regarding claim 1, Shipp shows a method comprising

receiving an email message from a simple mail transfer protocol (SMTP) server, the email message comprising ([0018,0023])

a text body ([0064,0065])

an SMTP email address ([0018,0023,0039,0045,0046])

a domain name corresponding to the SMTP email address ([0039,0045,0046])

an attachment ([0081])

tokenizing the text body to generate tokens representative of words in the text ([0064-0067])

tokenizing the SMTP email address to generate a token representative of the SMTP email address ([0039,0043,0069])

tokenizing the domain name to generate a token that is representative domain name ([0022])

as well as showing MD5 hasing ([0093]).

Shipp does not show a 32-bit string indicative of the length of the email message, nor does Shipp show tokenizing the attachment and the steps comprising tokenizing said attachment, determining a probability value for each generated token, selecting a predefined number of interesting tokens, the interesting tokens being the generated tokens having the greatest non-neutral probability value; performing a Bayesian analysis on the selected interesting tokens to generate a spam probability; and categorizing the email message as a function of the generated spam probability.

Devine shows utilizing a 32-bit string in a message header which is indicative of the total length of said message (col. 24 lines 52-67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp with that of Devine in order to better identify message contents so as to facilitate leveraging common code for processing messages (Devine col. 23 lines 60-61).

Shipp in view of Devine do not show tokenizing the attachment.

Milliken shows tokenizing the attachment to generate a token that is representative of the attachment, the tokenizing steps comprising the steps of generating a MD5 hash of the attachment ([0010-0013 and 0052]where MD5 hashes are inherently 128-bit).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine with that of Milliken in order to better identify spam email, as at the time of Shipp's disclosure, spam email was thought "currently" not to be associated with attachments ([81]), an area for which Milliken's more recent disclosure provides updated guidance.

Shipp in view of Devine and Milliken do not show appending the 32-bit string to the generated MD5 hash to produce a 160-bit number.

Anderson shows ([0057-0059]) appending an MD5 hash (inherently 128-bits) to network transmission size information (shown by Devine to be said 32-bit string, and where 32 +128 is inherently 160).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine and Milliken with that of

Anderson in order to better uniquely identify messages (Anderson [0057-0059]), leading to improved message spam identification.

Shipp in view of Devine, Milliken and Anderson do not show UUencoding said 160-bit number to generate a token representative of the attachment.

Uuencode and MIME FAQ shows UUencoding a file.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken and Anderson with that of Uuencode and MIME FAQ in order to store the message identification information (represented by the 160-bit number shown by Shipp in view of Devine, Milliken and Anderson) in a format easily exchanged over email (UUencode and MIME FAQ) since UUencoding produces an easily emailed file and since the disclosure of Shipp in view of Devine, Milliken and Anderson relates to email and files transferred over email. Furthermore, UUencoding is a prior art element, as shown in UUencode and MIME FAQ, and thus UUencoding the 160-bit number is combing a prior art element (UUencoding) to known methods (the known methods shown by Shipp in view of Devine, Milliken and Anderson) to yield predictable results (the results being a UUencoded item).

Shipp in view of Devine, Milliken, Anderson and UUencode and MIME FAQ do not show determining a probability value for each of the generated tokens.

Gordon shows determining a probability value for each of the generated tokens (col. 11 lines 15 –55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken, Anderson and Uuencode and MIME FAQ with that of Gordon in order to better identify spam elements in messages (Gordon col. 11 lines 15 –55).

Shipp in view of Devine, Milliken, Anderson, UUencode and MIME FAQ and Gordon do not show selecting a predefined number of interesting tokens, the interesting tokens being the generated tokens having the greatest non-neutral probability value; performing a Bayesian analysis on the selected interesting tokens to generate a spam probability; and categorizing the email message as a function of the generated spam probability.

Sahami shows selecting a predefined number of interesting tokens, the interesting tokens being the generated tokens having the greatest non-neutral probability value; performing a Bayesian analysis on the selected interesting tokens to generate a spam probability; and categorizing the email message as a function of the generated spam probability (pg. 2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken, Anderson, Uuencode and MIME FAQ and Gordon with that of Sahami in order to more accurately identify spam email.

Shipp in view of Devine, Milliken, Anderson, Uuencode and MIME FAQ, Gordonm and Shami thus show claim 1.

7. Claims 6, 16, 17, 23, 24, 25, 30, 31, 32, 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shipp in view of Milliken.

8. Regarding claims 6 Shipp shows a method comprising receiving an email message comprising a text body ([0064,0065]), an SMTP email address ([0039.0043,0069]), and a domain name corresponding to the SMTP email address ([0039,0045,0046]);

tokenizing the SMTP email address to generate a token representative of the SMTP email address ([0039,0043,0063])

tokenizing the domain name to generate a token representative of the domain name ([0022]), and determining a spam probability from the generated tokens ([0014,0076]).

Shipp does not show tokenizing the attachment to generate a token that is representative of the attachment.

Milliken shows tokenizing the attachment to generate a token that is representative of the attachment ([10-13 and 51 – 53]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp with that of Milliken in order to better identify spam email, as at the time of Shipp's disclosure, spam email was thought "currently" not to be associated with attachments ([81]); spam and attachments are however an area for which Milliken's more recent disclosure provides updated guidance.

9. Regarding claim 16, Shipp in view of Milliken further show receiving an email message including a text body (Shipp [0064,0065]).

10. Regarding claim 17, Shipp in view of Milliken further show tokenizing the words in the text body to generate tokens representative of the words in the text body (Shipp [0064,0065]).

11. Regarding claim 23, Shipp in view of Milliken further show a system comprising a text body (Shipp, [0064,0065]), an SMTP email address (Shipp, [0039.0043,0069]), and a domain name corresponding to the SMTP email address (Shipp, [0039,0045,0046]) and an attachment (Milliken [10-13]);

tokenizing the SMTP email address to generate a token representative of the SMTP email address (Shipp, [0039,0043,0063])

tokenizing logic configured to tokenize the attachment to generate a token that is representative of the attachment (Milliken [10-13 and 51 – 53])

tokenizing the domain name to generate a token representative of the domain name (Shipp, [0022]), and

determining a spam probability from the generated tokens (Shipp, [0014,0076]).

12. Regarding claim 24, Shipp in view of Milliken further show means for receiving an SMTP email address, and a domain name corresponding to the SMTP email address (Shipp, [0039,0045,0046]) and an attachment (Milliken [10-13]);

means for tokenizing the SMTP email address to generate a token representative of the SMTP email address (Shipp, [0039,0043,0063])

means for tokenizing logic configured to tokenize the attachment to generate a token that is representative of the attachment (Milliken [10-13 and 51 – 53])

means for tokenizing the domain name to generate a token representative of the domain name (Shipp, [0022]), and

means for determining a spam probability from the generated tokens (Shipp, [0014,0076]).

13. Regarding claim 25, Shipp in view of Milliken further show a computer-readable medium comprising computer-readable code adapated to instruct a programmable device to receiving an email message comprising an an SMTP email address, ([0039.0043,0069]), a domain name corresponding to the SMTP email address ([0039,0045,0046]) and an attachment (Milliken [10-13]);

tokenizing the SMTP email address to generate a token representative of the SMTP email address ([0039,0043,0063])

tokenizing logic configured to tokenize the attachment to generate a token that is representative of the attachment (Milliken [10-13 and 51 – 53])

tokenizing the domain name to generate a token representative of the domain name ([0022]), and

determining a spam probability from the generated tokens ([0014,0076]).

14. Regarding claim 30, Shipp in view of Milliken further show a system comprising email logic configured to receive an email message comprising an attachment (Shipp [0018,0023] and Milliken [10-13])),

tokenize logic configured to tokenize the entire attachment to generate a token representative of the attachment (Milliken [10-13 and 70]); and

analysis logic configured to determine a spam probability from the generated token (Milliken [10-13] and Shipp [14,76]).

15. Regarding claim 31, Shipp in view of Milliken further show means for receiving an email message comprising an attachment (Shipp [0018,0023] and Milliken [10-13])),

means for tokenizing the attachment to generate a token representative of the attachment (Milliken [10-13 and 70]); and

means for determining a spam probability from the generated token (Milliken [10-13] and Shipp [14,76]).

16. Regarding claim 32, Shipp in view of Milliken further show a computer-readable medium comprising computer-readable code adapted to instruct a programmable device to receive an email message comprising an attachment (Shipp [0018,0023] and Milliken [10-13])),

computer-readable code adapted to instruct a programmable device to tokenize logic configured to tokenize the entire attachment to generate a toke representative of

the attachment (Milliken [10-13 and 70]); and

computer-readable code adapted to instruct a programmable device to determine a spam probability from the generated token (Milliken [10-13] and Shipp [14,76]).

17. Regarding claim 33, Shipp in view of Milliken further show receiving an email message including a text body (Shipp [0064,0065]).

18. Regarding claim 34, Shipp in view of Milliken further show tokenizing the words in the text body to generate tokens representative of the words in the text body (Shipp [0064,0065]).

19. Claims 11, 12, 13,14, 19, 20, 21, 22, 26, 27, 28, 29, 35, 36, 37, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shipp in view of Milliken as applied to claims 6 and 25 above, and further in view of Gordon and Sahami.

13. Regarding claims 11 and 26, Shipp in view of Milliken show assigning a spam probability value, including considering the token representative of the SMTP email address (Shipp [0018,0023,0039,0040-0043]) and the token representative of the domain name (Shipp [0022]).

Shipp in view of Milliken do not show where spam probability values are assigned to individual tokens, but rather shows utilizing an aggregate value based on all tokens.

Gordon shows assigning probability values to individual tokens (col. 11 lines 15 – 55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Milliken with that of Gordon in order to better identify spam elements in messages (Gordon col. 11 lines 15 –55).

Shipp in view of Milliken and Gordon do not show generating a Bayesian probability values using the spam probability values assigned to the tokens.

Sahami shows generating a Bayesian probability values using the spam probability values assigned to the tokens (pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Milliken and Gordon with that of Sahami in order to more accurately identify spam email.

14. Regarding claims 12 and 27 Shipp in view of Milliken, Gordon and Sahami further show comparing the generated Bayesian probability value with a predefined threshold value (Sahami, pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

15. Regarding claims 13 and 28 Shipp in view of Milliken, Gordon and Sahami further show categorizing the email message as spam in response to the Bayesian probability value being greater than the predefined threshold (Sahami, pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

16. Regarding claims 14 and 29 Shipp in view of Milliken, Gordon and Sahami further show categorizing the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold (Sahami pg. 6 col. 1).

17. Regarding claims 19 and 35, Shipp in view of Milliken show claim 17 and 34.

Shipp in view of Milliken do not show assigning a spam probability value to each of the tokens representation of the words in the text body nor due they show assigning a spam probability value specifically to the attachment, but rather determining a single spam probability value utilizing the tokens.

Gordon shows (Gordon, col. 11 lines 15 – 55), assigning a spam probability value to the token to each of the tokens representative of the words in the text body, and to the token representative of the attachment (Gordon, col. 11 lines 15 –55, Milliken [0010-0013]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Milliken with that of Gordon in order to better identify spam elements in messages (Gordon col. 11 lines 15 –55).

Shipp in view of Milliken and Gordon do not show generating a Bayesian probability value using the spam probability values assigned to the token.

Shamai shows generating a Bayesian probability value using the spam probability values assigned to the token (Sahami, pg. 4 col. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Milliken and Gordon with that of Sahami in order to more accurately identify spam email.

18. Regarding claims 20 and 36, Shipp in view of Milliken, Gordon and Sahami further show comparing the generated Bayesian probability value with a predefined threshold value (Sahami, pg. 4 col. 2).

19. Regarding claims 21 and 37, Shipp in view of Milliken, Gordon and Sahami further show categorizing the email message as spam in response to the Bayesian probability value being greater than the predefined threshold (Sahami, pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

20. Regarding claims 22 and 38, Shipp in view of Milliken, Gordon and Sahami further show categorizing the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold (Sahami, pg. 6 col. 1).

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN M. FRINK whose telephone number is (571)272-

9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John Frink

(571) 272 - 9686

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2142